REMARKS

I. Introduction

In response to the Office Action dated March 1, 2004, please consider the following remarks. Claims 1-42 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. The Cited References and the Subject Invention

A. The Kocher Reference

U.S. Patent No. 6,289,455 issued September 11, 2001 to Kocher et al. disclose a method and apparatus for preventing piracy of digital content. A secure cryptographic rights unit for cryptographically regulating access to digital content includes an interface control processor and a specialized cryptographic unit that protects access to a memory. Rights keys, which allow access to content, are added by the cryptographic unit by transforming data received from the control processor and storing the result in the protected memory. The cryptographic unit then produces content decryption keys by using stored rights keys to transform other data received from the control processor. Because the control processor does not have the ability to directly access the protected memory, the security can remain effective even if the control processor is compromised. To prevent reverse engineering of the cryptographic transformations, the invention provides for an algorithm generator that uses random sources to produce algorithm definitions in machine-readable form. Because the generator itself does not contain any secrets, it can be submitted for open review.

B. The Sims Reference

U.S. Patent No. 6,550,011, issued April 15, 2003 to Sims discloses a media content protection utilizing public key cryptography. A system and method for providing protection of content which may be transmitted over unsecure channels, including storage and transmission in bulk media, transmission over a network such as the Internet, transmission between components of an open system, and broadcast transmitted, to compliant storage devices and/or compliant use devices is disclosed. The technique for providing protection from unauthorized utilization of the content so stored is provided publicly in order to allow for those utilizing a conforming media

device to master or generate content protected according to the present invention. According to a preferred embodiment, public key cryptography is utilized to identify compliant devices and to transmit cryptographic keys protecting content data. In the preferred embodiment content is protected using private key cryptography to optimize system performance.

III. Office Action Prior Art Rejections

In paragraphs (3)-(4), the Office Action rejected claims 1-15 and 17-41 under 35 U.S.C. § 102(e) as anticipated over Kocher et al., U.S. Patent No. 6,289,455 (Kocher). The Applicants respectfully traverse these rejections.

With Respect to Claims 1 and 28: Claim 1 recites:

> *A method of storing program material for subsequent replay, comprising the steps of:*
> *(a) accepting encrypted access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and control data;*
> *(b) decrypting the received access control information to produce the first encryption key;*
> *(c) decrypting the program material using the first encryption key;*
> *(d) re-encrypting the program material according to a second encryption key;*
> *(e) encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and*
> *(f) providing the re-encrypted program material and the fourth encryption key for storage.*

According to the Office Action, the features recited in the Applicants' preamble, *"a method of storing program material for subsequent replay"* is discloses at col. 5, lines 55-65 of the Kocher reference as follows:

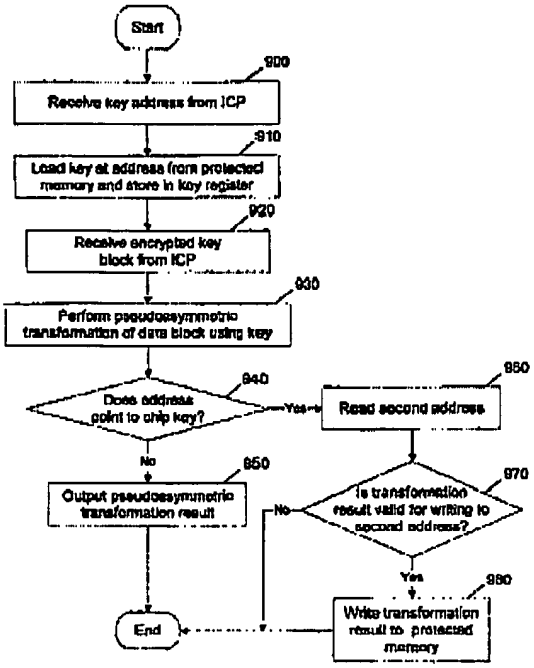
> The present invention can improve the security of systems used to distribute and protect digital content. One embodiment of the invention, in a tamper-resistant device for regulating access to encoded digital content, includes an external interface, a microprocessor for controlling the external interface, a memory, a cryptographic unit connected between the microprocessor and memory configured to protect the memory from the microprocessor by cryptographically transforming data communicated between the microprocessor and the memory, and a device key accessible by the cryptographic unit and inaccessible by the microprocessor. The device is configured such that the cryptographic

Because the foregoing does not disclose storing program material for subsequent replay, the Applicants respectfully disagree.

The Office Action indicates that the remaining features of claim 1 are disclosed in col. 16, line 47 through col. 17, line 10, and in FIG. 9 as follows:

FIG. 9 diagrams the operation of an exemplary CryptoFirewall that implements prepaid rights but can be easily extended to support post-paid rights. The nonvolatile protected memory behind the CryptoFirewall contains a device key (CHIP_KEY) as well as memory locations for storing prepaid rights keys. At step **900**, the CryptoFirewall receives a key address from the ICP and makes sure that the address corresponds to a valid key offset in the protected memory. (For example, if keys are 8 bytes long, zeroing the three least significant address bits ensures that the base address is not mis-aligned.) At step **910**, the CryptoFirewall loads from the protected memory the data stored at the specified address and places the result in a key register. At step **920**, the CryptoFirewall receives a data block from the ICP. At step **930**, the CryptoFirewall uses the key read at step **910** with a pseudoasymmetric function to transform the data block obtained at step **920**. At step **940**, the CryptoFirewall tests whether if the address read at step **900** corresponds to the location of the CHIP_KEY in the protected memory. If not, at step **950**, the CryptoFirewall outputs the pseudoasymmetric transformation result to the ICP and concludes. (Results produced using keys other than CHIP_KEY—i.e., rights keys—are used to derive content decryption keys, so the results are not stored. Transformations protected with the CHIP_KEY are used to add new rights keys to the protected memory.) Otherwise, at step **960**, the CryptoFirewall reads a second address from the ICP. At step **970**, the CryptoFirewall optionally tests whether the result of the transformation is valid for writing at the address specified at step **960** to prevent attackers from inappropriately modifying values in the protected memory. This check is primarily required to prevent over-writing of CHIP_KEY values stored in updateable memory. (For example, before allowing a write to the CHIP_KEY, the CryptoFirewall can verify that the result of the pseudoasymmetric transformation has a predefined characteristic—for example, that its first 56 bits equal "10" repeated 28 times.) Alternatively or in addition, the CryptoFirewall should verify that the destination address value is appropriate (e.g., not pointing to the CHIP_KEY). If the CryptoFirewall determines at step **970** that the write is authorized, it performs the write at step **980**.

FIGURE 9



The foregoing appears to disclose merely the use of a CHIP_KEY stored in secure memory to decrypt a datablock from the ICP. Referring to FIG. 9 and the related text:

Block 900 discloses receiving a key address. It does not disclose the step of *receiving encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data.* It therefore does not disclose the features of paragraph (a) of claim 1.

Block 930 appears to disclose a decryption operation of a data block, not *access control information to produce an encryption key.* It therefore fails to disclose the features of paragraph (b) of claim 1.

Block 950 discloses outputting the result of block 930 (a decryption operation of a data block) if the address does not point to the CHIP_KEY. It does not disclose *encrypting the second encryption key according to a third encryption key to produce a fourth encryption key.*

Block 910 discloses a storing operation, but it does not disclose *providing the re-encrypted program material and the fourth encryption key for storage.* Indeed, since it preceeds the operations shown in block 920, it cannot possibly do so, even if the foregoing blocks in FIG. 9 disclose what the Office Action alleges.

Finally, block 590 discloses using a content decryption key to decrypt content, but this operation is performed in connection with different procedures (FIG.5) than that which is disclosed and above with respect to the remaining features of claim 1 (FIG. 9).

Accordingly, the Applicants respectfully traverse the rejection of claim 1.

Claim 28 recites features analogous to those of claim 1 and is patentable on the same basis.

With Respect to Claim 2: Claim 2 recites:

> *The method of claim 1, wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of:*
> *decrypting the received access control information to produce the temporally-variant control data; and*
> *modifying the temporally variant control data to generate temporally-invariant control data.*

According to the Office Action, these features are disclosed as follows:

> **17**
> produced using keys other than CHIP_KEY—i.e., rights keys—are used to derive content decryption keys, so the results are not stored. Transformations protected with the CHIP_KEY are used to add new rights keys to the protected memory.) Otherwise, at step **960**, the CryptoFirewall reads

As described below, a "rights key" is a key that is needed to decrypt and obtain content decryption keys.

Rights Key: A value (such as a cryptographic key) that allows a CRU to generate or decode the decryption keys for some content. Rights keys are generally required to decrypt KDMs and obtain content decryption keys.

Therefore, the Kocher reference discloses that the chip key is used to add new rights to the protected memory, and that those rights keys are used to decrypt (key derivation messages) KDMs to obtain content decryption keys decryption keys that are used to decrypt content. The Applicants do not understand how the foregoing reasonably discloses decrypting temporally variant control data and modifying the temporally variant control data to generate temporally-invariant control data. In particular, there does not appear to be a *modifying* step at all.

With Respect to Claims 5, 6, 20, and 21: Claim 5 recites that the access control information further comprises metadata describing at least one right for the program material. The Office Action indicates that the Kocher's statement "that implements prepaid rights but can be easily extended to support post-paid rights" (col. 16, lines 47-49) teaches these features, but the Applicants respectfully disagree. The foregoing statement in Kocher merely states that rights can be pre-paid or post-paid. The Applicants respectfully submit that this does not disclose access control information comprising metadata describing at least one right for the program material.

The Office Action also asserts that the foregoing statement in Kocher teaches *generating the second encryption key at least in part from the metadata.* The Applicants respectfully disagree. As far as is ascertainable, Kocher does not teach generating any encryption keys from metadata, let alone metadata received as a part of received access control information.

Claims 6, 20, and 21 are patentable under the same rationale.

With Respect to Claims 8 and 9: Claims 8 and 9 recite the step of generating replay right data from the metadata. Kocher does not disclose using metadata to generate play rights, let alone replay rights.

With Respect to Claims 10 and 11: Claims 10 and 11 recite steps involving the retrieval of the reencrypted and stored program material, and decrypting it according to a fourth key that is decrypted using a third key. None of these features are even remotely suggested by the Kocher reference.

With Respect to Claims 12 and 13: Claim 12 recites:

The method of claim 11, wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the method further comprises the steps of:

generating replay right data from the metadata;

accepting the buy data;

comparing the buy data with the replay right data; and

decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data.

According to the Office Action, the foregoing is discloses in the Kocher reference with the statement "rights keys are used to derive content decryption keys, so the results are not stored. Transformation protected with the CHIP_KEY are used to add new rights keys." The Applicants respectfully disagree. The foregoing passage does not disclose replay rights, metadata describing replay rights, or the comparison of buy data with replay right data. Accordingly, the Applicants respectfully traverse this rejection.

Claim 13 recites further features and is even more remote from the Kocher reference.

With Respect to Claim 14-15: As far as the applicants can ascertain, Kocher does not teach re-encrypting program material, a fourth encryption key, nor storing either in a media storage device.

With Respect to Claim 17: Claim 17 recites:

An apparatus for storing program material encrypted according to a first encryption key for replay, comprising:

a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising:

a first decryption module, for decrypting the access control information to produce the first encryption key;

a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and

a second decryption module for decrypting the fourth encryption key to produce the second encryption key.

The Office Action erroneously refers to claim 17 as a dependent claim, and erroneously indicates that claim 17 recites "a tuner". The Applicants respectfully traverse this rejection, and respectfully request that if the claim remains rejected in a subsequent and non-Final Office Action, that a specific rationale for the rejection of this claim be specified. Although many of the features of

claim 17 are not present in the Kocher reference, the Applicants suggest that particular attention be paid to the first encryption module recited in claim 17.

With Respect to Claim 18: The Applicants respectfully disagree that claim 18 incorporates substantially the same subject material as claim 17, as it also recites a third decryption module, a second encryption module, and a fourth decryption module, all of which are not disclosed in the Kocher reference.

With Respect to Claim 19: According to the Office Action, claim 19 incorporates substantially similar subject matter as claim 7. The Applicants respectfully disagree. Although they both recite a pre-buy module (which is not disclosed in the Kocher reference), they claim different subject matter.

With Respect to Claim 22: The cited portion of the Kocher reference "When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)" does not disclose a communicatively coupled "buy" and "pre buy" module.

With Respect to Claims 23 and 24: Claim 23 recites:

> *The apparatus of claim 22, wherein the buy module comprises:*
> *a purchase module for accepting buy data and comparing the buy data and the replay right data from the pre-buy module; and*
> *a control module for controlling the second decryption module based on the comparison between the buy data and the replay right data.*

According to the Office Action, these features are disclosed by the statement "A communications channel from the CRU 225 to content provider 200 is also provided for auditing post-payment purchases." However, this only discloses providing data regarding payment after view purchases to the content provider. It does not disclose replay right data or controlling a decryption module based on a comparison between the buy data and the replay right data.

With Respect to Claims 29-41: Claims 29-41 recite features analogous to those of claims 2-16 and is patentable on the same basis.

In paragraphs (5)-(6), the Office Action rejected claims 16 and 42 under 35 U.S.C. §103(a) as being unpatentable over Kocher as applied to claims above in further view of Sims, III, U.S. Patent No. 6,550,011 B1 (Sims). Applicants respectfully traverse these rejections.

With Respect to Claim 16: The Office Action acknowledges that the Kocher reference does not teach "wherein the temporally-variant control data associates an expiration time with the program material", but suggests these features are taught in col. 11 lines 33-41 of the Sims reference as follows:

> A preferred embodiment compliant information use device also includes secure areas, such as a portion of storage area **113**, for storing content use information. Such information may include a generation counter, generation limit, copyright status indication, expiration information, watermark verification data, region coding, byte count limits, time limits, expiration based on the end of the content, and the like. Moreover, if the information use

Presumably, the Office Action is referring to the "time limits" or "expiration information", or "expiration based on the end of content" phrases.

The Office Action also indicates that:

> "It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of protecting digital content used in distribution taught in '455 to include a method for extending the expiration time. One of ordinary skill in the art would have been motivated to perform such a modification because a need exist for a more versatile method to allow distribution and protect content see '011 (col. 3, lines 55 et seq.) 'Likewise, a need exists in the art for a more robust set of rules establishing authorized utilization of content"

Of course, the mere statement that a more robust set of rules is needed does not itself teach the expiration of the user's right to view content. Further, the Applicants respectfully disagree that there is any teaching to modify Kocher. In fact, Kocher itself teaches away from the modification suggested in the Office Action. Specifically, Kocher teaches that if viewing rights are to have a temporal component, those rights should be enforced by canceling and changing over keys, as shown in col. 25 lines 43-58, reproduced below:

> Content providers should change rights keys periodically to ensure that users who have lost their authorization cannot access content. For example, if a user terminates a subscription, the CRU may continue to operate unless the rights key is deleted/disabled or mechanisms outside the CryptoFirewall disable access. Content providers can limit the maximum duration of such use by making rights keys expire periodically (e.g., hourly, daily, weekly, monthly, annually, etc.) To ensure that key changeovers do not disrupt legitimate viewers, new rights keys can be distributed before the old ones are discontinued. During the changeover period, content can also be broadcast with KDMs that can operate using both the old rights key and the new one. An additional option is to queue the REM that updates the key until the key change is required. (Such queuing can be done by the playback device, ICP, etc.)

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the Applicants. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicants. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994).

Based on the foregoing, Kocher itself teaches away from the modification suggested by the Office Action. Accordingly the Applicants respectfully traverse this rejection.

IV. Dependent Claims

Dependent claims 2-16, 18-27, and 29-42 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

V. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: June 1, 2004

By: Victor G. Cooper
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/amb